

Applicant : Peter D. Baker, et al.
Appl. No. : 10/715,954
Examiner : Jude Jean Giles
Docket No. : 705593.4001

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

1. (currently amended) A method of securely distributing digital content, comprising: receiving a content distribution request from a content user; retrieving a digital content item in response to the content distribution request; generating on demand a first encryption algorithm for encrypting the digital content item; configuring a protocol parsing engine to encrypt the digital content item, using the first encryption algorithm; encrypting the digital content item using the configured protocol parsing engine; and transmitting the encrypted digital content item to the content user.
2. (original) The method of claim 1, further comprising generating a first encryption key.
3. (original) The method of claim 2, wherein the configuring step further comprises using the first encryption key.
4. (original) The method of claim 1, further comprising recording an encryption identifier adapted to identify the first encryption algorithm.
5. (original) The method of claim 1, wherein the first encryption algorithm is different from a second encryption algorithm, the second encryption algorithm being a previously generated encryption algorithm used to encrypt a second digital content item transmitted to a second content user.
6. (original) The method of claim 1, wherein generating the encryption algorithm comprises retrieving the encryption algorithm from a pool of encryption algorithms.

| | | |
|------------|---|------------------------|
| Applicant | : | Peter D. Baker, et al. |
| Appl. No. | : | 10/715,954 |
| Examiner | : | Jude Jean Giles |
| Docket No. | : | 705593.4001 |

7. (currently amended) A method of securely accessing encrypted digital content, comprising: requesting from a content provider access to encrypted digital content; receiving decryption information comprising a decryption algorithm generated on demand from the content provider; decrypting the encrypted digital content using the decryption information; accessing the decrypted digital content; and deleting the decryption information.

8. (original) The method of claim 7, wherein the encrypted digital content is stored locally.

9. (original) The method of claim 7, wherein the decryption information comprises an executable decryption code module.

10. (original) The method of claim 9, wherein the executable decryption code module is created on demand by the content provider.

11. (original) The method of claim 10, wherein the executable decryption code module is created by a protocol description configured to generate executable code.

12. (original) The method of claim 7, wherein the received decryption information is stored in volatile memory.

13. (original) The method of claim 7, wherein the decrypted digital content is stored in volatile memory.

14. (original) The method of claim 7, further comprising deleting the decrypted digital content once it has been accessed.

15. (original) The method of claim 7, further comprising receiving encryption information from the content provider and re-encrypting the decrypted digital content, using the

Applicant : Peter D. Baker, et al.
Appl. No. : 10/715,954
Examiner : Jude Jean Giles
Docket No. : 705593.4001

encryption information.

16. (original) The method of claim 15, wherein the encryption information is different from second encryption information used to initially encrypt the decrypted digital content.

17. (currently amended) A method of providing secure access to encrypted digital content, comprising: receiving a request to access encrypted digital content; retrieving generating on demand a decryption algorithm for decrypting the encrypted digital content; configuring a protocol description to generate a code module for decrypting the encrypted digital content, using the decryption algorithm; generating the code module for decrypting the encrypted digital content, using the configured protocol description; transmitting the code module to the content user.

18. (original) The method of claim 17, wherein the code module comprises an executable code module.

19. (original) The method of claim 17, wherein the request to access encrypted digital content comprises an identifier identifying the digital content.

20. (original) The method of claim 19, wherein retrieving the decryption algorithm comprises regenerating a decryption algorithm, based on the identifier.